DATA SHARING AGREEMENT
FOR
CONFIDENTIAL INFORMATION OR LIMITED DATASET(S)
BETWEEN
STATE OF WASHINGTON
DEPARTMENT OF HEALTH
AND

Snohomish County

This Agreement documents the conditions under which the Washington State Department of Health (DOH) shares confidential information or limited Dataset(s) with other entities.

CONTACT INFORMATION FOR ENTITIES RECEIVING AND PROVIDING INFORMATION

	INFORMATION RECIPIENT	INFORMATION PROVIDER
Organization Name	Snohomish County	Washington State Department of Health (DOH)
Tax ID Number	91-6001368	
Business Contact Name	Pam Aguilar	Jim Jansen
Title	Deputy Department Director	WEMSIS Data System Manager
Address	3020 Rucker Ave Suite 306 Everett, WA 98201	PO Bx 47853 Olympia, WA 98504-7890
Telephone #	425-339-8690	360-236-2821
Email Address	Pamela.aguilar@snoco.org	Jim.jansen@doh.wa.gov
IT Security Contact	Jim Kamp	John Weeks
Title	Business Management Analyst	Chief Information Security Officer
Address	3020 Rucker Ave Suite 306 Everett, WA 98201	PO Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8689	360-999-3454
Email Address	Jim.kamp@co.snohomish.wa.us	Security@doh.wa.gov
Privacy Contact Name	Jannah Abdul-Qadir	Michael Paul
Title	Privacy and Public Records Officer	DOH Chief Privacy Officer
Address	3020 Rucker Ave Suite 306 Everett, WA 98201	P. O. Box 47890 Olympia, WA 98504-7890
Telephone #	425-339-8641	(564) 669-9692
Email Address	Jannah.abdul-qadir@co.snohomish.wa.us	Privacy.officer@doh.wa.gov

DEFINITIONS

Authorized user means a recipient's employees, agents, assigns, representatives, independent contractors, or other persons or entities authorized by the data recipient to access, use or disclose information through this agreement.

Authorized user agreement means the confidentiality agreement a recipient requires each of its Authorized Users to sign prior to gaining access to Public Health Information.

Breach of confidentiality means unauthorized access, use or disclosure of information received under this agreement. Disclosure may be oral or written, in any form or medium.

Breach of security means an action (either intentional or unintentional) that bypasses security controls or violates security policies, practices, or procedures.

Confidential information means information that is protected from public disclosure by law. There are many state and federal laws that make different kinds of information confidential. In Washington State, the two most common are the Public Records Act RCW 42.56, and the Healthcare Information Act, RCW 70.02.

Data storage means electronic media with information recorded on it, such as CDs/DVDs, computers and similar devices.

Data transmission means the process of transferring information across a network from a sender (or source), to one or more destinations.

Direct identifier Direct identifiers in research data or records include names; postal address information (other than town or city, state and zip code); telephone numbers, fax numbers, e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate /license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

Disclosure means to permit access to or release, transfer, or other communication of confidential information by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record.

Encryption means the use of algorithms to encode data making it impossible to read without a specific piece of information, which is commonly referred to as a "key". Depending on the type of information shared, encryption may be required during data transmissions, and/or data storage.

Health care information means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care…." RCW 70.02.010(7)

Health information is any information that pertains to health behaviors, human exposure to environmental contaminants, health status, and health care. Health information includes health care information as defined by RCW 70.02.010 and health related data as defined in RCW 43.70.050.

Human subjects research; human subject means a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information.

Identifiable data or records contains information that reveals or can likely associate the identity of the person or persons to whom the data or records pertain. Research data or records with direct identifiers removed, but which retain indirect identifiers, are still considered identifiable.

Indirect identifiers are indirect identifiers in research data or records that include all geographic identifiers smaller than a state , including street address, city, county, precinct, Zip code, and their equivalent postal codes, except for the initial three digits of a ZIP code; all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such age and elements may be aggregated into a single category of age 90 or older.

Limited dataset means a data file that includes potentially identifiable information. A limited dataset does not contain direct identifiers.

Potentially identifiable information   means information that includes indirect identifiers which may permit linking an individual to that person's health care information. Examples of potentially identifiable information include:
- birth dates;
- admission, treatment or diagnosis dates;
- healthcare facility codes;
- other data elements that may identify an individual. These vary depending on factors such as the geographical location and the rarity of a person's health condition, age, or other characteristic.

Restricted confidential information   means confidential information where especially strict handling requirements are dictated by statutes, rules, regulations or contractual agreements. Violations may result in enhanced legal sanctions.

State holidays State legal holidays, as provided in RCW 1.16.050.

GENERAL TERMS AND CONDITIONS

I. USE OF INFORMATION

The Information Recipient agrees to strictly limit use of information obtained or created under this Agreement to the purposes stated in Exhibit I (and all other Exhibits subsequently attached to this Agreement). For example, unless the Agreement specifies to the contrary the Information Recipient agrees not to:

- Link information received under this Agreement with any other information.
- Use information received under this Agreement to identify or contact individuals.

The Information Recipient shall construe this clause to provide the maximum protection of the information that the law allows.

II. SAFEGUARDING INFORMATION

A. CONFIDENTIALITY

Information Recipient agrees to:

- Follow DOH small numbers guidelines as well as dataset specific small numbers requirements. (Appendix D)

- Limit access and use of the information:
  - To the minimum amount of information .
  - To the fewest people.
  - For the least amount of time required to do the work.

- Ensure that all people with access to the information understand their responsibilities regarding it.

- Ensure that every person (e.g., employee or agent) with access to the information signs and dates the "Use and Disclosure of Confidential Information Form" (Appendix A) before accessing the information.
  - Retain a copy of the signed and dated form as long as required in Data Disposition Section.

The Information Recipient acknowledges the obligations in this section survive completion, cancellation, expiration or termination of this Agreement.

B. SECURITY

The Information Recipient assures that its security practices and safeguards meet Washington State Office of the Chief Information Officer (OCIO) security standard 141.10 *Securing Information Technology Assets*.

For the purposes of this Agreement, compliance with the HIPAA Security Standard and all subsequent updates meets OCIO standard 141.10 "Securing Information Technology Assets."

The Information Recipient agrees to adhere to the Data Security Requirements in Appendix B. The Information Recipient further assures that it has taken steps necessary to prevent unauthorized access, use, or modification of the information in any form.

Note: The DOH Chief Information Security Officer must approve any changes to this section prior to Agreement execution. IT Security Officer will send approval/denial directly to DOH Contracts Office and DOH Business Contact.

C. BREACH NOTIFICATION

The Information Recipient shall notify the DOH Chief Information Security Officer (security@doh.wa.gov) within one (1) business days of any suspected or actual breach of security or confidentiality of information covered by the Agreement.

III. **RE-DISCLOSURE OF INFORMATION**

Information Recipient agrees to not disclose in any manner all or part of the information identified in this Agreement except as the law requires, this Agreement permits, or with specific prior written permission by the Secretary of the Department of Health.

If the Information Recipient must comply with state or federal public record disclosure laws, and receives a records request where all or part of the information subject to this Agreement is responsive to the request: the Information Recipient will notify the DOH Privacy Officer of the request ten (10) business days prior to disclosing to the requestor. The notice must:

- Be in writing;

- Include a copy of the request or some other writing that shows the:
    - Date the Information Recipient received the request; and
    - The DOH records that the Information Recipient believes are responsive to the request and the identity of the requestor, if known.

IV.   ATTRIBUTION REGARDING INFORMATION

Information Recipient agrees to cite "Washington State Department of Health" or other citation as specified, as the source of the information subject of this Agreement in all text, tables and references in reports, presentations and scientific papers.

Information Recipient agrees to cite its organizational name as the source of interpretations, calculations or manipulations of the information subject of this Agreement.

V.   OTHER PROVISIONS

With the exception of agreements with British Columbia for sharing health information, all data must be stored within the United States.

VI.   AGREEMENT ALTERATIONS AND AMENDMENTS

This Agreement may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties

VII.   CAUSE FOR IMMEDIATE TERMINATION

The Information Recipient acknowledges that unauthorized use or disclosure of the data/information or any other violation of sections II or III, and appendices A or B, may result in the immediate termination of this Agreement.

VIII.   CONFLICT OF INTEREST

The DOH may, by written notice to the Information Recipient:

Terminate the right of the Information Recipient to proceed under this Agreement if it is found, after due notice and examination by the Contracting Office that gratuities in the form of entertainment, gifts or otherwise were offered or given by the Information Recipient, or an agency or representative of the Information Recipient, to any officer or employee of the DOH, with a view towards securing this Agreement or securing favorable treatment with respect to the awarding or amending or the making of any determination with respect to this Agreement.

In the event this Agreement is terminated as provided in the paragraph above, the DOH shall be entitled to pursue the same remedies against the Information Recipient as it could pursue in the event of a breach of the Agreement by the Information Recipient. The rights and remedies of the DOH provided for in this section are in addition to any other rights and remedies provided by law. Any determination made by the Contracting Office under this clause shall be an issue and may be reviewed as provided in the "disputes" clause of this Agreement.

IX.   DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the DOH and the Information Recipient and it cannot be resolved, either party may submit a request for a dispute resolution to the Contracts and Procurement Unit. The parties agree that this resolution process shall precede any action in a judicial and quasi-judicial tribunal. A party's request for a dispute resolution must:

- Be in writing and state the disputed issues, and

- State the relative positions of the parties, and

- State the information recipient's name, address, and his/her department agreement number, and

- Be mailed to the DOH contracts and procurement unit, P. O. Box 47905, Olympia, WA 98504-7905 within thirty (30) calendar days after the party could reasonably be expected to have knowledge of the issue which he/she now disputes.

This dispute resolution process constitutes the sole administrative remedy available under this Agreement.

X.   EXPOSURE TO DOH BUSINESS INFORMATION NOT OTHERWISE PROTECTED BY LAW AND UNRELATED TO CONTRACT WORK

During the course of this contract, the information recipient may inadvertently become aware of information unrelated to this agreement. Information recipient will treat such information respectfully, recognizing DOH relies on public trust to conduct its work. This information may be handwritten, typed, electronic, or verbal, and come from a variety of sources.

XI.   GOVERNANCE

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of Washington and any applicable federal laws. The provisions of this Agreement shall be construed to conform to those laws.

In the event of an inconsistency in the terms of this Agreement, or between its terms and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

- Applicable Washington state and federal statutes and rules;

- Any other provisions of the Agreement, including materials incorporated by reference.

XII.   **HOLD HARMLESS**

Each party to this Agreement shall be solely responsible for the acts and omissions of its own officers, employees, and agents in the performance of this Agreement. Neither party to this Agreement will be responsible for the acts and omissions of entities or individuals not party to this Agreement. DOH and the Information Recipient shall cooperate in the defense of tort lawsuits, when possible.

XIII.   **LIMITATION OF AUTHORITY**

Only the Authorized Signatory for DOH shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this Agreement on behalf of the DOH. No alteration, modification, or waiver of any clause or condition of this Agreement is effective or binding unless made in writing and signed by the Authorized Signatory for DOH.

XIV.   **RIGHT OF INSPECTION**

The Information Recipient shall provide the DOH and other authorized entities the right of access to its facilities at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this Agreement on behalf of the DOH.

XV.   **SEVERABILITY**

If any term or condition of this Agreement is held invalid, such invalidity shall not affect the validity of the other terms or conditions of this Agreement, provided, however, that the remaining terms and conditions can still fairly be given effect.

XVI.   **SURVIVORSHIP**

The terms and conditions contained in this Agreement which by their sense and context, are intended to survive the completion, cancellation, termination, or expiration of the Agreement shall survive.

XVII.   **TERMINATION**

Either party may terminate this Agreement upon 30 days prior written notification to the other party. If this Agreement is so terminated, the parties shall be liable only for performance rendered or costs incurred in accordance with the terms of this Agreement prior to the effective date of termination.

XVIII.   **WAIVER OF DEFAULT**

This Agreement, or any term or condition, may be modified only by a written amendment signed by the Information Provider and the Information Recipient. Either party may propose an amendment.

Failure or delay on the part of either party to exercise any right, power, privilege or remedy provided under this Agreement shall not constitute a waiver. No provision of this Agreement may be waived by either party except in writing signed by the Information Provider or the Information Recipient.

XIX.   **ALL WRITINGS CONTAINED HEREIN**

This Agreement and attached Exhibit(s) contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement and attached Exhibit(s) shall be deemed to exist or to bind any of the parties hereto.

XX.   **PERIOD OF PERFORMANCE**

This **Agreement** shall be effective from date of signature through 6/30/2027.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date of last signature below.

INFORMATION PROVIDER   **INFORMATION RECIPIENT**

State of Washington Department of Health   Snohomish County Health Department

_____   _____
Signature   Signature

_____   _____
Print Name   Print Name

_____   _____
Date   Date

EXHIBIT I

1. **PURPOSE AND JUSTIFICATION FOR SHARING THE DATA**

   Provide a detailed description of the purpose and justification for sharing the data, including specifics on how the data will be used.

   Data recipient will utilize this data in two main ways. Firstly, it will serve as input for the comprehensive analysis of violence across Snohomish County within the broader Cardiff model framework. The Information Recipient plans to integrate this data into a visual map, plotting where events took place throughout Snohomish County and overlaying various community resources to determine proximity to care. The Information Recipient hopes to gain deeper insights into the nature and distribution of violence within the community. Achieving this will necessitate precise location information to integrate with various other data streams, such as hospitalization records, mortality statistics, and law enforcement data. This analysis aims to drive resource allocation and inform public health decisions by identifying violence hotspots and service gaps. The results will be used to optimize the deployment of community resources, improve access to care, and develop targeted violence prevention strategies.

   Secondly, these data will contribute to a county-wide report focusing on injury and violence among youth and young adults in Snohomish County. Recipient will present estimates at the census block level (or tract or zip code where appropriate) regarding incidents attended by EMS personnel, with appropriate measures taken to suppress data for small numbers. This will be coupled with insights from a range of supplementary data sources. Additionally, recipient will provide details on the characteristics of these incidents, including the type of weapon involved, age groups affected, and gender distribution. Consideration will also be given to evaluating the inclusion of additional characteristics such as race.
   Data may be shared publicly in adherence with DOH small numbers guidelines and RCW 70.168.090 and will not identify any health information at the patient, provider, or facility level.

   The report will primarily be for internal use and will comply with RCW 70.168.090 and RCW 70.02.010 definitions for de-identified data, as well as the stipulations for disclosure. Data, including census tract and zip code information, will be used internally to gain deeper insights into the distribution and nature of violence in Snohomish County. For public sharing, data will be de-identified by removing census tract and zip code information, along with any other indirect identifiers that could potentially lead to the identification of a patient, provider, or facility. Data will also be presented in aggregate form, with appropriate measures taken to suppress small numbers to prevent identification.
   For internal purposes, census tract and zip code data will be used to enhance the analysis and drive resource allocation and public health decisions. This report can only be distributed to individuals who need the report for business purposes such as public health action. Public sharing of the report will adhere to DOH small numbers guidelines, ensuring that no health information at the patient, provider, or facility level is disclosed.

Is the purpose of this agreement for human subjects research that requires Washington State Institutional Review Board (WSIRB) approval?

☐ Yes ☒ No

If yes, has a WSIRB review and approval been received? If yes, please provide copy of approval. If No, attach exception letter.

☐ Yes ☐ No

2. PERIOD OF PERFORMANCE

This **Exhibit I** shall have the same period of performance as the **Agreement** unless otherwise noted below:

Exhibit ____ shall be effective from_____through_____.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement:
Database Name(s): Washington Emergency Medical Services Information System
Data Selection Criteria: Provided annually, records for individuals who have an injury inflicted upon them, i.e. are involved in an assault either as a perpetrator or a victim or unknown. Complaint reported by Dispatch (eDispatch.01); all assaults, stab/gunshot wounds/penetrating trauma.
Data Elements being provided: *provide all data elements to be shared here. Attachments are not recommended.*

Gender (ePatient.13)
Race (ePatient.14)
Age (ePatient.15) although can use categorized age groups, such as <30, 30-59, 60+
Type of Other Service at Scene (eScene.04)
Scene GPS location (eScene.11)
Street address (eScene.15)
City (eScene.17)
State (eScene.18)
Census Tract (eScene.23)
Date/time of symptom onset (eSituation.01)
Possible Injury (eSituation.02)
Complaint type (eSituation.03)
Complaint (eSituation.04)
Chief Complaint Anatomic Location (eSituation.07)

Primary Symptom (eSituation.09)
Provider's Primary Impression (eSituation.11)
Initial Patient Acuity (eSituation.13)
Cause of Injury (eInjury.01)
Mechanism of Injury (eInjury.02)
Trauma Center Criteria (eInjury.03)
Patient Care report narrative (eNarrative.01)
Incident Patient Disposition (eDisposition.12)
Reason for Refusal/release (eDisposition.31)

The information described in this section is:

- ☒ Restricted Confidential Information (Category 4)
- ☐ Confidential Information (Category 3)
- ☐ Potentially identifiable information (Category 3)
- ☐ Internal [public information requiring authorized access] (Category 2)
- ☐ Public Information (Category 1)

Any reference to data/information in this Agreement shall be the data/information as described in this Exhibit.

4. STATUTORY AUTHORITY TO SHARE INFORMATION

DOH statutory authority to obtain and disclose the confidential information or limited Dataset(s) identified in this Exhibit to the Information Recipient:

RCW 70.02.050 – Disclosure without patient's authorization
RCW 70.168.090 – Statewide data registry—Statewide electronic emergency medical services data system—Quality assurance program—Confidentiality.

Information Recipient's statutory authority to receive the confidential information or limited Dataset(s) identified in this Exhibit:

RCW 70.168.090 – Statewide data registry—Statewide electronic emergency medical services data system—Quality assurance program—Confidentiality.
RCW 70.05.070 – Local health officer—Powers and duties.

5. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

☐ DOH Web Application (indicate application name):

☒ Washington State Managed File Transfer (https://mftprod-server.watech.wa.gov)

☐ Encrypted CD/DVD or other storage device

☐ Health Information Exchange (HIE)**

☐ Other: (describe the methods for access/transfer)**

NOTE: DOH Chief Information Security Officer must approve prior to Agreement execution. DOH Chief Information Security Officer will send approval/denial directly to DOH Contracts Office and DOH Business Contact.

FREQUENCY OF ACCESS/TRANSFER

☐ One time: DOH shall deliver information by _____ (insert date)

☒ Repetitive: Annually

☐ As available within the period of performance stated in Section 2.

6. REIMBURSEMENT TO DOH

Payment for services to create and provide the information is based on the actual expenses DOH incurs, including charges for research assistance when applicable.

Billing Procedure

- Information Recipient agrees to pay DOH by check or account transfer within 30 calendar days of receiving the DOH invoice.

- Upon expiration of the Agreement, any payment not already made shall be submitted within 30 days after the expiration date or the end of the fiscal year, which is earlier.

Charges for the services to create and provide the information are:

☐ $_____

☒ No charge.

7. DATA DISPOSITION

Unless otherwise directed in writing by the DOH Business Contact, at the end of this Agreement, or at the discretion and direction of DOH, the Information Recipient shall:

☒ Immediately destroy all copies of any data provided under this Agreement after it has been used for the purposes specified in the Agreement . Acceptable methods of destruction are described in Appendix B. Upon

completion, the Information Recipient shall submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☐   Immediately return all copies of any data provided under this Agreement to the DOH Business Contact after the data has been used for the purposes specified in the Agreement, along with the attached Certification of Data Disposition (Appendix C)

☐   Retain the data for the purposes stated herein for a period of time not to exceed _____ (*e.g., one year, etc*.), after which Information Recipient shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☐   Other (Describe):

8. RIGHTS IN INFORMATION

Information Recipient agrees to provide, if requested, copies of any research papers or reports prepared as a result of access to DOH information under this Agreement for DOH review prior to publishing or distributing.

In no event shall the Information Provider be liable for any damages, including, without limitation, damages resulting from lost information or lost profits or revenue, the costs of recovering such Information, the costs of substitute information, claims by third parties or for other similar costs, or any special, incidental, or consequential damages, arising out of the use of the information. The accuracy or reliability of the Information is not guaranteed or warranted in any way and the information Provider's disclaim liability of any kind whatsoever, including, without limitation, liability for quality, performance, merchantability and fitness for a particular purpose arising out of the use, or inability to use the information.

☐ If checked, please submit the following:

- Copies of _____ (insert list of items)_____
  to the attention of: ___(insert name of DOH employee) __
  at ___(insert address to which material is sent)_____ .

9. ALL WRITINGS CONTAINED HEREIN

This Agreement and attached Exhibit(s) contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this

Agreement and attached Exhibit(s) shall be deemed to exist or to bind any of the parties hereto.

IN WITNESS WHEREOF, the parties have executed this Exhibit as of the date of last signature below.

INFORMATION PROVIDER

State of Washington Department of Health

_____
Signature

_____
Print Name

_____
Date

INFORMATION RECIPIENT

Snohomish County Health Department

_____
Signature

_____
Print Name

_____
Date

EXHIBIT II

1. PURPOSE AND JUSTIFICATION FOR SHARING THE DATA

Provide a detailed description of the purpose and justification for sharing the data, including specifics on how the data will be used.

WEMSIS Quarterly County Opioid Analytic Dataset
The purpose of this data is to inform local approaches to county level opioid responses in compliance with RCW 70.168.090(2). Uses may include special studies and analysis consistent with requirements for confidentiality of patient and quality assurance. Use of the data for research is not permitted under this agreement.

This level of data is needed to identify areas in Snohomish County with higher rates of opioid responses to better address the local public health approach and resource allocation. This data will not be linked to any other data sources. Data will only be used by Snohomish County staff for informing public health interventions.

WEMSIS data that contains a patient's, provider's or facilities health outcome data is considered confidential per RCW 70.168.090. Confidentiality considerations should be made for all these parties.

Is the purpose of this agreement for human subjects research that requires Washington State Institutional Review Board (WSIRB) approval?

☐ Yes ☒ No

If yes, has a WSIRB review and approval been received? If yes, please provide copy of approval. If No, attach exception letter.

☐ Yes ☐ No

2. PERIOD OF PERFORMANCE

This Exhibit I shall have the same period of performance as the Agreement unless otherwise noted below:

Exhibit shall be effective from _____ through_____.

3. DESCRIPTION OF DATA

Information Provider will make available the following information under this Agreement:

Database Name(s): *Washington Emergency Medical Services Information System (WEMSIS)*
Online Report Name: *(County) Opioid Analytic Dataset*
Data criteria: *Records meeting the following case definition:*
   WEMSIS records in which:
      eScene21: Incident County is equal to "INSERT COUNTY NAME" or eScene.19: Incident
         ZIP code is a ZIP code entirely contained in "INSERT COUNTY NAME"; and
      eInjury.01: Cause of Injury contains an opioid related cause of injury; or
         eSituaiton.11: Primary impression is opioid related; or
         eSituaiton.12: Secondary Impression is opioid related; or
         eMedications.03 indicates Naloxone (Narcan) administration, and eMedications.07:
            Response to Medication is "Improved"

Data Elements being provided:

Data Element	Description
Incident Date	Date of the EMS response in MM/DD/YYYY format, based on NEMSIS field eTimes.03
Opioid Surveillance Report Deduplication ID	ID number created in the monthly opioid report to identify record from the same patient incident; see report for more details
Opioid Impression	Indicator for whether a opioid related ICD-10 code was recorded in the impressions or cause of injury in any EMS record matched to this patient
Suspected Overdose	Indicator for whether this record meets the condition of "Opioid Impression" or "Improved Naloxone Response"
Naloxone administered	Indicator for whether Naloxone administration was documented, either in the Narrative or the Medication fields
Improved Naloxone Response	Indicator for whether Naloxone was administered and a response of "Improved" was documented in any EMS record matched to this patient
Naloxone dose	Doses for Naloxone administration documented in the Medication fields
Naloxone admin route	Route for Naloxone administration documented in the Medication fields
Naloxone administered prior to EMS arrival	Indicator for whether Naloxone was administered prior to the arrival of EMS
Role of person administering Naloxone	Role of person who administered Naloxone prior to EMS arrival, based on NEMSIS field eMedications.10
Naloxone left at scene	Whether Naloxone was left at scene, according to the designated field in the record

Death before or during response	Indicator for whether the patient was dead before or at the end of the EMS response
Suspected Opioid Related Incident	Custom ImageTrend field for whether it is a suspected opioid related incident
Transported to a medical facility	Indicator for whether the patient was transported to a medical facility, based on NEMSIS fields eDisposition.01 and eDisposition.21
Reason refused transport	NEMSIS field eDisposition.31
Primary Symptom	NEMSIS field eSituation.09
Secondary Symptoms	NEMSIS field eSituation.10
Provider's Primary Impression	NEMSIS field eSituation.11
Provider's Secondary Impressions	NEMSIS field eSituation.12
Incident Location Type	Type of scene of the incident in ICD-10 code Y92 format, NEMSIS field eScene.09
Incident Street Address	NEMSIS field eScene.15
Incident Location County	County in WA of the scene of the incident, incorporating entries in eScene.17, eScene.19, and eScene.21 where necessary
Incident Location ZIP	Postal code of the scene of the incident, NEMSIS field eScene.19
Incident Location census tract	NEMSIS field eScene.23
Destination Facility Name	Destination facility name, NEMSIS field eDisposition.01
Age	Age of the patient in years at the time of the incident, according to the documented Age and Age Units, or the difference in years between Date of Birth and the Incident Date
Gender	Gender of the patient, NEMSIS field ePatient.13
Race	Race and/or ethnicity of the patient, NEMSIS field ePatient.14
Patient Residence County	County in which the patient resides, not restricted to WA, NEMSIS field ePatient.07
Patient Residence ZIP	Postal code in which the patient resides, not restricted to WA, NEMSIS field ePatient.09
Patient Residence Census Tract	NEMSIS field ePatient.11
Patient Housing Status	Indicator for whether the patient was reported as homeless in either ePatient.05 or ePatient.22
EMS Service Name	EMS service name of the responding EMS unit, NEMSIS field dAgency.03
Type of Other Service at Scene	NEMSIS field eScene.04
Response Time to Scene	Difference between entries in NEMSIS fields eTimes.03 and eTimes.06

The information described in this section is:

☒ Restricted Confidential Information (Category 4)
☐ Confidential Information (Category 3)
☐ Potentially identifiable information (Category 3)
☐ Internal [public information requiring authorized access] (Category 2)
☐ Public Information (Category 1)

Any reference to data/information in this Agreement shall be the data/information as described in this Exhibit.

10. STATUTORY AUTHORITY TO SHARE INFORMATION

DOH statutory authority to obtain and disclose the confidential information or limited Dataset(s) identified in this Exhibit to the Information Recipient:

RCW 43.70.050 – Collection, use, and accessibility of health-related data
RCW 70.168.090 - Statewide data registry—Statewide electronic emergency medical services data system—Quality assurance program—Confidentiality.

Information Recipient's statutory authority to receive the confidential information or limited Dataset(s) identified in this Exhibit:
RCW 70.168.090 - Statewide data registry—Statewide electronic emergency medical services data system—Quality assurance program—Confidentiality.
RCW 70.05.070 – Local health officer—Powers and duties.

11. ACCESS TO INFORMATION

METHOD OF ACCESS/TRANSFER

☐ DOH Web Application (indicate application name):
☒ Washington State Managed File Transfer (https://mftprod-server.watech.wa.gov)
☐ Encrypted CD/DVD or other storage device
☐ Health Information Exchange (HIE)**
☐ Other: Encrypted email

**NOTE: DOH Chief Information Security Officer must approve prior to Agreement execution. DOH Chief Information Security Officer will send approval/denial directly to DOH Contracts Office and DOH Business Contact.

FREQUENCY OF ACCESS/TRANSFER

    ☐   One time: DOH shall deliver information by   _____   (insert date)

    ☒   Repetitive: Quarterly through the end of 2027.

    ☐   As available within the period of performance stated in Section 2.

12. REIMBURSEMENT TO DOH

Payment for services to create and provide the information is based on the actual expenses DOH incurs, including charges for research assistance when applicable.

Billing Procedure

- Information Recipient agrees to pay DOH by check or account transfer within 30 calendar days of receiving the DOH invoice.

- Upon expiration of the Agreement, any payment not already made shall be submitted within 30 days after the expiration date or the end of the fiscal year, which is earlier.

Charges for the services to create and provide the information are:

    ☐ $_____

    ☒   No charge.

13. DATA DISPOSITION

Unless otherwise directed in writing by the DOH Business Contact, at the end of this Agreement, or at the discretion and direction of DOH, the Information Recipient shall:

    ☐   Immediately destroy all copies of any data provided under this Agreement after it has been used for the purposes specified in the Agreement . Acceptable methods of destruction are described in Appendix B. Upon completion, the Information Recipient shall submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

    ☐   Immediately return all copies of any data provided under this Agreement to the DOH Business Contact after the data has been used for the purposes specified in the Agreement, along with the attached Certification of Data Disposition (Appendix C)

☒ Retain the data for the purposes stated herein for a period of time not to exceed one year, after which Information Recipient shall destroy the data (as described below) and submit the attached Certification of Data Disposition (Appendix C) to the DOH Business Contact.

☐ Other (Describe):

14. RIGHTS IN INFORMATION

Information Recipient agrees to provide, if requested, copies of any research papers or reports prepared as a result of access to DOH information under this Agreement for DOH review prior to publishing or distributing.

In no event shall the Information Provider be liable for any damages, including, without limitation, damages resulting from lost information or lost profits or revenue, the costs of recovering such Information, the costs of substitute information, claims by third parties or for other similar costs, or any special, incidental, or consequential damages, arising out of the use of the information. The accuracy or reliability of the Information is not guaranteed or warranted in any way and the information Provider's disclaim liability of any kind whatsoever, including, without limitation, liability for quality, performance, merchantability and fitness for a particular purpose arising out of the use, or inability to use the information.

☐ If checked, please submit the following:

- Copies of _____ (insert list of items)_____
  to the attention of: ___(insert name of DOH employee) __
  at ____(insert address to which material is sent)_____ .

15. ALL WRITINGS CONTAINED HEREIN

This Agreement and attached Exhibit(s) contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement and attached Exhibit(s) shall be deemed to exist or to bind any of the parties hereto.

IN WITNESS WHEREOF, the parties have executed this Exhibit as of the date of last signature below.

INFORMATION PROVIDER   **INFORMATION RECIPIENT**

State of Washington Department of Health   Snohomish County Health Department

_____   _____
Signature   Signature

_____   _____
Print Name   Print Name

_____   _____
Date   Date

APPENDIX A

<u>USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION</u>

People with access to confidential information are responsible for understanding and following the laws, policies, procedures, and practices governing it. Below are key elements:

A.   CONFIDENTIAL INFORMATION
Confidential information is information federal and state law protects from public disclosure. Examples of confidential information are social security numbers, and healthcare information that is identifiable to a specific person under RCW 70.02. The general public disclosure law identifying exemptions is RCW 42.56.

B.   ACCESS AND USE OF CONFIDENTIAL INFORMATION
    1.   Access to confidential information must be limited to people whose work specifically requires that access to the information.
    2.   Use of confidential information is limited to purposes specified elsewhere in this Agreement.

C.   DISCLOSURE OF CONFIDENTIAL INFORMATION
    1.   An Information Recipient may disclose an individual's confidential information received or created under this Agreement to that individual or that individual's personal representative consistent with law.
    2.   An Information Recipient may disclose an individual's confidential information, received or created under this Agreement only as permitted under the ***Re-Disclosure of Information*** section of the Agreement, and as state and federal laws allow.

D.   CONSEQUENCES OF UNAUTHORIZED USE OR DISCLOSURE
An Information Recipient's unauthorized use or disclosure of confidential information is the basis for the Information Provider immediately terminating the Agreement. The Information Recipient may also be subject to administrative, civil and criminal penalties identified in law.

E.   ADDITIONAL DATA USE RESTRICTIONS: (if necessary)
To maintain confidentiality, WEMSIS users shall
- Use WEMSIS only for Quality Improvement, service monitoring, public health surveillance and related activities.
- Immediately report inadvertent disclosure of personal health information to the WEMSIS Administrator (WEMSIS@doh.wa.gov)
- Not use WEMSIS for personal use.
- Publish output from WEMSIS in a manner that assures confidentiality of the patient, provider and EMS service and adhere to the Department of Health small numbers

guidelines when publishing or distributing information on very small groups: small numbers guidelines.

- Take reasonable precautions to prevent unauthorized access to the WEMSIS system, such as testing and installing security patch updates, using complex passwords, using workstation locks such as password protected screensavers, closing WEMSIS when leaving workstation, and not sharing user IDs and passwords.
- Take reasonable precautions to avoid unauthorized access to WEMSIS output, such as removing paper output from public areas and using caution when transmitting output electronically.
- Notify WEMSIS Administrator (WEMSIS@doh.wa.gov) of access changes (e.g. separation from employment)
- Not grant access to individuals without first submitting a WEMSIS Confidentiality Agreement to the WEMSIS Administrator (WEMSIS@doh.wa.gov).

Signature: _____

Date:_____

APPENDIX B

<u>DATA SECURITY REQUIREMENTS</u>

Protection of Data

The storage of Category 3 and 4 information outside of the State Governmental Network requires organizations to ensure that encryption is selected and applied using industry standard algorithms validated by the NIST Cryptographic Algorithm Validation Program. Encryption must be applied in such a way that it renders data unusable to anyone but authorized personnel, and the confidential process, encryption key or other means to decipher the information is protected from unauthorized access. All manipulations or transmissions of data within the organizations network must be done securely.

The Information Recipient agrees to store information received under this Agreement (the data) within the United States on one or more of the following media, and to protect it as described below:

A. Passwords

1. Passwords must always be encrypted. When stored outside of the authentication mechanism, passwords must be in a secured environment that is separate from the data and protected in the same manner as the data. For example passwords stored on mobile devices or portable storage devices must be protected as described under section *F. Data storage on mobile devices or portable storage media*.

2. Complex Passwords are:

   * At least 8 characters in length.
   * Contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
   * Do not contain the user's name, user ID or any form of their full name.
   * Do not consist of a single complete dictionary word but can include a passphrase.
   * Do not consist of personal information (e.g., birthdates, pets' names, addresses, etc.).
   * Are unique and not reused across multiple systems and accounts.
   * Changed at least every 120 days.

B. Hard Disk Drives / Solid State Drives – Data stored on workstation drives:

1. The data must be encrypted as described under section *F. Data storage on mobile devices or portable storage media*. Encryption is not required when Potentially Identifiable Information is stored temporarily on local workstation Hard Disk Drives/Solid State Drives. Temporary storage is thirty (30) days or less.

2. Access to the data is restricted to authorized users by requiring logon to the local workstation using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts and remain locked for at least 15 minutes, or require administrator reset.

C. Network server and storage area networks (SAN)

1. Access to the data is restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network.

2. Authentication must occur using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

3. The data are located in a secured computer area, which is accessible only by authorized personnel with access controlled through use of a key, card key, or comparable mechanism.

4. If the servers or storage area networks are not located in a secured computer area **or** if the data is classified as Confidential or Restricted it must be encrypted as described under *F. Data storage on mobile devices or portable storage media*.

D. Optical discs (CDs or DVDs)

1. Optical discs containing the data must be encrypted as described under *F. Data storage on mobile devices or portable storage media*.

2. When not in use for the purpose of this Agreement, such discs must be locked in a drawer, cabinet or other physically secured container to which only authorized users have the key, combination or mechanism required to access the contents of the container.

E. Access over the Internet or the State Governmental Network (SGN).

1. When the data is transmitted between DOH and the Information Recipient, access is controlled by the DOH, who will issue authentication credentials.

2. Information Recipient will notify DOH immediately whenever:

   a) An authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Information Recipient;

b) Whenever a person's duties change such that the person no longer requires access to perform work for this Contract.

3. The data must not be transferred or accessed over the Internet by the Information Recipient in any other manner unless specifically authorized within the terms of the Agreement.

    a) If so authorized the data must be encrypted during transmissions using a key length of at least 128 bits. Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required.

    b) Authentication must occur using a unique user ID and Complex Password (of at least 10 characters). <u>When the data is classified as Confidential or Restricted</u>, authentication requires secure encryption protocols and multi-factor authentication mechanisms, such as hardware or software tokens, smart cards, digital certificates or biometrics.

    c) Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

F. Data storage on mobile devices or portable storage media

1. Examples of mobile devices are: smart phones, tablets, laptops, notebook or netbook computers, and personal media players.

2. Examples of portable storage media are: flash memory devices (e.g. USB flash drives), and portable hard disks.

3. The data must not be stored by the Information Recipient on mobile devices or portable storage media unless specifically authorized within the terms of this Agreement. If so authorized:

    a) The devices/media must be encrypted with a key length of at least 128 bits, using industry standard mechanisms validated by the National Institute of Standards and Technologies (NIST).

        • Encryption keys must be stored in a secured environment that is separate from the data and protected in the same manner as the data.

    b) Access to the devices/media is controlled with a user ID and a Complex Password (of at least 6 characters), or a stronger authentication method such as biometrics.

    c) The devices/media must be set to automatically <u>wipe</u> or be rendered unusable after no more than 10 failed access attempts.

d) The devices/media must be locked whenever they are left unattended and set to lock automatically after an inactivity activity period of 3 minutes or less.

e) The data must not be stored in the Cloud. This includes backups.

f) The devices/ media must be physically protected by:

- Storing them in a secured and locked environment when not in use;
- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.

4. When passwords and/or encryption keys are stored on mobile devices or portable storage media they must be encrypted and protected as described in this section.

G. Backup Media

The data may be backed up as part of Information Recipient's normal backup process provided that the process includes secure storage and transport, and the data is encrypted as described under *F. Data storage on mobile devices or portable storage media.*

H. Paper documents

Paper records that contain data classified as Confidential or Restricted must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records is stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

I. Data Segregation

1. The data must be segregated or otherwise distinguishable from all other data. This is to ensure that when no longer needed by the Information Recipient, all of the data can be identified for return or destruction. It also aids in determining whether the data has or may have been compromised in the event of a security breach.

2. When it is not feasible or practical to segregate the data from other data, then ***all*** commingled data is protected as described in this Exhibit.

J. Data Disposition

If data destruction is required by the Agreement, the data must be destroyed using one or more of the following methods:

Data stored on:	Is destroyed by:
Hard Disk Drives / Solid State Drives	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, or
	Degaussing sufficiently to ensure that the data cannot be reconstructed, or
	Physically destroying the disk , or
	Delete the data and physically and logically secure data storage systems that continue to be used for the storage of Confidential or Restricted information to prevent any future access to stored information. One or more of the preceding methods is performed before transfer or surplus of the systems or media containing the data.
Paper documents with Confidential or Restricted information	On-site shredding, pulping, or incineration, or
	Recycling through a contracted firm provided the Contract with the recycler is certified for the secure destruction of confidential information.
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a course abrasive.
Magnetic tape	Degaussing, incinerating or crosscut shredding.
Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data.
	Physically destroying the disk.
	Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed.

K. Notification of Compromise or Potential Compromise

The compromise or potential compromise of the data is reported to DOH as required in Section II.C.

APPENDIX C

<u>CERTIFICATION OF DATA DISPOSITION</u>

Date of Disposition _____

☐   All copies of any Datasets related to agreement DOH#_____ have been deleted from all data storage systems. These data storage systems continue to be used for the storage of confidential data and are physically and logically secured to prevent any future access to stored information. Before transfer or surplus, all data will be eradicated from these data storage systems to effectively prevent any future access to previously stored information.

☐   All copies of any Datasets related to agreement DOH#_____ have been eradicated from all data storage systems to effectively prevent any future access to the previously stored information.

☐   All materials and computer media containing any data related to agreement DOH #_____ have been physically destroyed to prevent any future use of the materials and media.

☐   All paper copies of the information related to agreement DOH #_____ have been destroyed on-site by cross cut shredding.

☐   All copies of any Datasets related to agreement DOH #_____ that have not been disposed of in a manner described above, have been returned to DOH.

☐   Other

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in agreement DOH # _____, Section J, Disposition of Information, have been fulfilled as indicated above.

_____   _____

Signature of data recipient   Date

APPENDIX D

<u>DOH SMALL NUMBERS GUIDELINES</u>

- Aggregate data so that the need for suppression is minimal. Suppress all non-zero counts which are less than ten.

- Suppress rates or proportions derived from those suppressed counts.

- Assure that suppressed cells cannot be recalculated through subtraction, by using secondary suppression as necessary. Survey data from surveys in which 80% or more of the eligible population is surveyed should be treated as non-survey data.

- When a survey includes less than 80% of the eligible population, and the respondents are unequally weighted, so that cell sample sizes cannot be directly calculated from the weighted survey estimates, then there is no suppression requirement for the weighted survey estimates.

- When a survey includes less than 80% of the eligible population, but the respondents are equally weighted, then survey estimates based on fewer than 10 respondents should be "top-coded" (estimates of less than 5% or greater than 95% should be presented as 0-5% or 95-100%).